STAT
Declassified in Part - Sanitized Copy Approved for Release 2012/12/11 :
CIA-RDP89B01354R000400480031-2

Page Denied

Declassified in Part - Sanitized Copy Approved for Release 2012/12/11 :
CIA-RDP89B01354R000400480031-2

Declassified in Part - Sanitized Copy Approved for Release 2012/12/11 : CIA-RDP89B01354R000400480031-2

Director of Central Intelligence
Security Committee
Computer Security Subcommittee

DCISEC-CSS-M175

1. The one hundred and seventy-fifth meeting of the Computer Security Subcommittee was convened on 15 October 1985 at the [redacted] The following persons attended the meeting: STAT

[redacted] Executive Secretary STAT
Mrs. Karen Deneroff, Dept. of State
Mr. Norman Clark, Navy
Mr. Richard Smith, Navy
Major Jack Freeman, Army
Mr. David Schenken, US Secret Service
[redacted] CIA STAT
Mr. Paul Fitzgerald, FBI
[redacted] NSA STAT
Mr. Robert Graytock, Dept. of Justice
Mr. Michael Bernott, Air Force
[redacted] SECOM
[redacted] IC Staff/IHC STAT
[redacted] IC Staff/IHC

2. The minutes of the previous minutes were reviewed. It was noted that Mr. Graytock was incorrectly listed as being from the Dept. of Treasury. He is, in fact, the member from the Dept. of Justice. A number of corrections and updates to the membership list were also received. The corrected membership list is attached.

3. The first discussion dealt with the issue of the Memorandum of Understanding (MOU) for facility approvals. Specifically, we discussed the paper, "Proposed Changes and Modifications to DCID 1/16, Computer Security Manual". Rather than dealing with the details of the MOU and the process for achieving joint accreditation of facilities, the discussion centered about the discrepancies between the formally defined accreditation process and how systems actually get "on the air" under current practice. The distinctions between initial operational approval and full certification and accreditation were discussed at length. Since the formally defined process is involved and lengthy, an informal process has evolved by which someone well below the DAA can grant an interim operational approval for a system, thus allowing it to operate without full accreditation. Since the interim approval process is informal, the "interim" status may, in fact, be indefinite. Thus, the result of this process is that a number of systems are currently operating which have never been, and never will be, formally accredited. It was argued that the currently defined accreditation process does not work; many systems are operating with only interim approval. On the other hand, if the defined process is strictly enforced, then needed operational capability will not be available due to the delays the process creates. Thus, the argument was for a well-defined and enforceable process for accreditation which recognizes the need for, and accomodates and regulates, the interim approval process. The membership next discussed. mechanisms for regulating and limiting the interim status. Mr.Clark and [redacted] agreed to prepare a strawman description of the interim approval process.

STAT

Declassified in Part - Sanitized Copy Approved for Release 2012/12/11 : CIA-RDP89B01354R000400480031-2

Declassified in Part - Sanitized Copy Approved for Release 2012/12/11 : CIA-RDP89B01354R000400480031-2

4. The next topic discussed was the work on the PC Security Guidelines, which has been contracted to the National Bureau of Standards. It was noted that there were three deliverables under this effort, the first of which was a user's brochure. A draft of this deliverable was distributed. The schedule was also reviewed. STAT

5. The status of the funding for R&D tasks was reviewed. There are essentially no funds for fy86. Apparently, the view is that the SECOM should provide seed money for selected projects which need a start, but that they should not be in the business of providing continuing funding of R&D programs. Long-term funding, it is felt, should be provided by a department or agency; the proper role of the SECOM is to fund new initiatives. Along a similar vein, [redacted] reported, in response to a previous inquery, that the Computer Security Center's R&D organization (i.e., C3) could respond to tasking from both the CSS and the civil agencies. However, it was noted that the Center has yet to receive R&D requirements from the civil agencies. The conclusion is that the CSS' perceived needs for Intel community computer security R&D can be communicated to the National Computer Security Center. It was felt that [redacted] was STAT the proper channel through which to communicate such requirements.

6. Miscellaneous items:

- [redacted] reported that the 2nd Annual Computer STAT Security Report is now being compiled by the NTISSC. Good cooperation is being experienced from the various participating agencies.

- Major Freeman reviewed some of the work on DoDD 5200.28 and 5200.28M. Current drafts include requirements from the Trusted Computer System Evaluation Criteria.

- John Lane will be leaving ASD($C^3I$), and will be going to the Department of Justice.

- Dave Jones has left the Department of Energy, joining the National Computer Security Center. He will be replaced by Mr. Leon Breault (sp ?).

7. The next meeting was set for 0930 on 12 November at the [redacted] STAT

STAT

[redacted]

Executive Secretary

Declassified in Part - Sanitized Copy Approved for Release 2012/12/11 : CIA-RDP89B01354R000400480031-2

STAT
Declassified in Part - Sanitized Copy Approved for Release 2012/12/11 : CIA-RDP89B01354R000400480031-2

Page Denied

Next 1 Page(s) In Document Denied

Declassified in Part - Sanitized Copy Approved for Release 2012/12/11 : CIA-RDP89B01354R000400480031-2